UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,571	01/12/2004	Kensaku Yamaguchi	247558US2RD	8239

22850 7590 10/12/2007

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
10/12/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/754,571	YAMAGUCHI ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-8 are pending. Claims 1-3 and 5-7 are amended.

Response to Arguments

Applicant's arguments, see page 6, filed 07/09/2007, with respect to the rejection(s) of claim(s) 1-8 under 102(b) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Shirakawa et al. hereafter Shirakawa (US 2002/0051536).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the condition wherein the keys do not match) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims use a conditional "if" statement and fail to mention what happens if the condition is not met.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8 rejected under 35 U.S.C. 103(a) as being unpatentable over Shirakawa.

Regarding claim 1:

Shirakawa discloses a tamper resistant microprocessor that executes a plurality of programs in parallel under a mult-task programming environment [paragraph 002], comprising:

a decryption unit [figure 1, 501 and 601] configured to read out an execution code or data [paragraph 40, 501 reads out an instruction and 601 reads out data] of one of a plurality of encrypted programs [paragraphs 2 and 6, it is inherent that the mult-task execution environment supports more that one program and that external memory would contain additional programs] and decrypt the execution code or data by using a prescribed encryption key corresponding to the read-out encrypted program, according to a decryption request from the cache memory control unit [paragraphs 74 and 75, instruction decryption processing unit 501 receives a read request from instruction cache 301; unit 501 decrypts the encrypted program data by applying the program key];

a cache memory [figure 1, 301 and 401] configured to store the execution code or data decrypted by the decryption unit [figure 1, 501 and 601; paragraphs 74-76] into

one of cache lines provided in the cache memory, the execution code or data stored in the cache memory remaining even after each program terminates [paragraphs 0074-76 cache replacement algorithms are well known in the art and the data in cache remains in the cache until it is replaced through the algorithm]; and

the cache memory control unit [figures 9 and 10, 504 and 604 respectively] configured to process a reading request for the execution code [paragraphs 74 and 75] or data [paragraphs 77 and 78] to be acquired from the decryption unit or the cache memory such that [paragraph 74, the control unit 504 controls the command data register and the decryption unit], the execution code or data in the cache memory is read out.

Shirawaka does not disclose each cache line containing a holding section for storing the encryption key used in decrypting the execution code or data, however, Shirawaka discloses a 'key pair tag' which is used as an index of the key pair table. It would have been obvious to one of ordinary skill in the art at the time of invention to store the key in the cache line as it would save time at the cost of storage as it is directly being read from the cache instead of being fetched every time. Furthermore, the alteration of Shirawaka discloses if the execution code or data exists in the cache memory and the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the prescribed key corresponding to a program that issues the reading request [paragraphs 94-98 and 108-116, it is obvious that the keys must match, else random, garbled information will be read out].

Regarding claim 2:

Shirawaka discloses the tamper resistant microprocessor of claim 1, further comprising:

a key value register configured to store the prescribed encryption key which is updated at an occasion executing each encrypted program [paragraphs 94-96, it is well known in the art that cache updates after each occasion of executing];

wherein the cache memory control unit judges whether the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the prescribed key stored in the key value register [paragraphs 110-116, tag judgement unit allows a transfer to occur if the key pair tag attached to the data matches the destination key pair tag].

Regarding claim 3:

Shirawaka discloses the tamper resistant microprocessor of claim 2, wherein the cache memory stores data decrypted by the decryption unit, and the cache memory control unit writes a processing result of the data into the cache memory, while storing the prescribed encryption key stored in the key value register into the secret protection attribute holding section of a cache line for the data [paragraphs 65-67, EX/MEM stage of the pipeline wherein the core would write to the cache memory].

Regarding claim 4:

Shirawaka discloses the tamper resistant microprocessor of claim 1, wherein the cache memory stores data decrypted by the decryption unit, and the cache memory control unit encrypts a processing result of the data by using the actual encryption key

stored in the secret protection attribute holding section of a cache line for the data, and writes encrypted data into an external memory device (paragraphs 81 and 82).

Regarding claims 5-8:

Claims 5-8 teach the method associated with the system disclosed in the rejection of claims 1-4.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100